Baker McKenzie.

Crypto Boot Camp 2022 Glossary

An A-Z of blockchain and crypto jargon

UNHASHING BLOCKCHAIN

Introduction

This glossary accompanies the Crypto Boot Camp 2022 virtual seminar series. The series will provide insights on how the regulatory landscape is changing and discuss the future of crypto within the financial services sector, including practical considerations when integrating crypto into established financial services, significant legal and regulatory risk, NFTs, DeFi and growth in the sector.

CLICK HERE

To register or for more information about the series

Index

No.

51% attack

A blockchain platform secured using a proof-of-work consensus protocol is generally protected from attack provided that honest nodes collectively control more mining power than any cooperating group of attacker nodes. A 51% attack is a situation where over half of the nodes on a blockchain network are controlled by a single malicious miner or a group of miners and such bad actors manipulate the blockchain to their own end (e.g., censoring transactions, including allowing double-spending. 51% attacks cannot steal coins as such because it is not possible to fake the signatures that secure transactions).

Aa

Address

An address is an alphanumeric character string, which can also be represented as a scannable QR code, that is used to send and receive transactions on a blockchain network. To send cryptocurrency to another person or platform, you will need their address (e.g., a cryptocurrency wallet has an address, as does an account on a cryptocurrency exchange).

Airdrop

A distribution of tokens free of charge to the cryptocurrency wallets of certain users, with or without advance notice. Typically carried out to reward loyal users, or create a buzz about a particular token.

Altcoin

A term used to describe cryptocurrency alternatives to Bitcoin such as Litecoin and Ether. Altcoins typically arise from forks of the Bitcoin software code rather than the Bitcoin blockchain itself (sometimes changing the number of coins, using a different hashing algorithm or adding some other new feature), but many innovative altcoins (e.g., Ethereum, Monero, NEO, IOTA, and others) use completely separate computer code and blockchains from Bitcoin.

Asset-backed tokens

Asset-backed tokens reflect an underlying physical asset such as gold.

Asset tokens

These tokens represent assets such as a debt or equity claim on the issuer, for example, a share in future company earnings or future capital flows, and may be tradable as investments.

ASIC

An "application-specific integrated circuit" — a silicon chip dedicated to a specific purpose rather than general purpose use, such as performing the hash algorithm, used to secure a proof-of-work blockchain. ASICs are more efficient at performing those specific purpose tasks than general purpose chips (it is now only viable to mine Bitcoin using an ASIC).

Atomic swap

An exchange of cryptocurrencies from separate blockchains without the use of a centralized intermediary such as an exchange. Such swaps are typically achieved using swap-enabled wallets and smart contracts.

Bb

Bag

A term used to refer to the holding of a significant quantity of a specific cryptocurrency by a person.

Bitcoin (BTC)

The first and best-known cryptocurrency created by Satoshi Nakamoto is a proof-of-work cryptocurrency facilitated by a blockchain.

Bits

A sub-unit of one Bitcoin. There are 1 million bits in one Bitcoin.

BIP

A "Bitcoin Improvement Proposal" — a technical design document providing information to the Bitcoin community, describing new proposed features, processes or environments affecting the Bitcoin protocol. Suggested changes to the protocol are submitted as a BIP. The BIP author is responsible for soliciting feedback.

Bitcoin maximalist

A person or entity that believes only the Bitcoin cryptocurrency deserves to survive long-term out of all cryptocurrencies on the market.

Block

Packages of data recorded on the blockchain. The block provides a lot of important information about the block, including its hash, the hash of the previous block, the nonce, timestamp, the difficulty and the block reward.

Blockspace

As block size is typically limited, there is a limit on the number of transactions that can be processed at a time. This creates a supply and demand market between miners, mining pools and users of a blockchain. The commodity of this market is often referred to as "blockspace," and is often in relation to where such blockspace is in high demand and thus at a premium cost in gas fees (e.g., as is the case with Ethereum blockspace).

Block explorer

An online tool that enables you to search for real-time current and historical information about a blockchain, including data related to blocks, transactions, addresses, hash rate and more.

Block height

The number of a given block, counted from the genesis block (sometimes referred to as "Block 0" or "Height 0").

Block reward

The reward that a miner receives for each new block that it mines (in the case of the Bitcoin blockchain, currently 6.25 BTC/block after having halved from 12.5 BTC in 2020).

Blockchain

A peer-to-peer, decentralized, immutable and distributed ledger that consists of validated blocks linked into a time-sequenced chain (imagine a spreadsheet that is not operated by a central party, but is operated by a network of computers and is designed to constantly refresh and update its content so that new entries are time-stamped and seen by all operators). The best-known blockchain is the Bitcoin blockchain.

Burn

Burning a token refers to the act of sending that token to an address that can only receive them. Wallet addresses used for burning cryptocurrency are called "burner" or "eater" addresses. The act of burning effectively removes tokens from the available supply, which decreases the number in circulation.

Cc

Chain tip

The most recent block added to a growing blockchain.

Chameleon hash (also referred to as "trapdoor hash functions")

A cryptographic hash function that could enable authorized administrators under an agreed governance model to edit or modify a transaction block in the blockchain without compromising the integrity of the blockchain.

Cold storage

The use of offline hardware devices to keep private keys used to access cryptocurrency offline in order to make it resistant to hacking, e.g., by using a USB drive (using software installed on the drive) or hardware wallet.

Consensus

An agreement between nodes in a DLT that the current state of the shared ledger is mathematically valid.

Corda

An open-source permissioned DLT platform created by R3.

Cryptoasset

A digital asset. Includes cryptocurrencies and tokens. Depending on the particular characteristics of the cryptoasset, it may or may not be a regulated product.

Cryptocurrency

A form of digital money that is exchanged via DLT. The most widely known cryptocurrency is Bitcoin (a number of policy-makers do not consider Bitcoin or other cryptocurrencies to meet the requirements of money in the traditional use of the word and so prefer the term cryptoasset).

Crypto trading bots

Automated cryptocurrency trading software that executes trade orders extremely quickly, based on a preset algorithm of buy-and-sell rules.

Dd

dApp

A "decentralized application" — an online software application created to run on DLT peer-to-peer networks, as opposed to centralized servers. Ethereum, EOS and NEO are popular open permissionless DLT networks for creating dApps.

DAO

A "decentralized autonomous organization" — an emerging type of digitally native organization governed not by traditional centralized governance structures (such as boards and executives), but rather by rules embedded in blockchain software code and enforced by the network of computers running such code. Members typically are able to participate by buying and holding the relevant token or cryptocurrency issued by the DAO with voting rights attached to them (usually proportional to their token holding), and voting on proposals made to the DAO. Often proposals can be made by any governance token holder, but increasingly holdings thresholds are set for very large DAOs. As DAOs are governed by code, execution of successful proposals can leverage integrated smart contracts, which are programmed to carry out certain activities on behalf of the DAO.

Decentralized exchange

A peer-to-peer exchange that allows users to buy and sell cryptocurrency and other cryptoassets without a central intermediary involved.

Decentralized finance (DeFi)

Blockchain-based financial services that do not rely on central financial intermediaries, i.e., brokerages, exchanges or banks, to offer traditional financial instruments. DeFi is an ecosystem of smart contracts, cryptoassets, stablecoins and other blockchain-native techniques and technologies that allow for peer-to-peer financial transactions and services, without the need for a third-party intermediary.

Difficulty

How hard it is to verify blocks in a blockchain network during proof-of-work mining. In Bitcoin's consensus mechanism, mining a block is difficult because the hash of a block's header must be lower than or equal to the target hash in order for the block to be accepted by the network. Put simply, the hash of a block must start with a certain number of zeros:

000000000000000000004e2123bdbd354a87cd51e176a2d- 3235e3d30ebd20045 — this is the hash of a block mined on 13 July 2018. As you can see, it has 20 zeros. Therefore, the probability of randomly selecting a nonce value that results in a hash that is less than or equal to the target value is very low. Therefore, many billions of different nonce values need to be tested. In the Bitcoin network, the difficulty of mining adjusts every 2016 blocks. This is to keep block verification time at 10 minutes.

Digital signature

A digital code that is created and validated by public key encryption, proving that only the holder of the private key could have generated the signature. This can be attached to a document sent electronically to identify the sender of the document, without revealing the sender's private key.

Distributed ledger technology (DLT)

A type of database that is distributed across multiple sites and network nodes and that is cryptographically secured. Blockchain is one type of DLT.

Double-spending problem

Given that digital information is so easily reproduced, once a digital currency is spent, how do you record this definitively? How can you prevent it getting spent more than once? This had been a longstanding concern with digital currencies.

Blockchain technology was invented to prevent double-spending without requiring a central trusted authority such as a bank.

Ee

EIP

An acronym for "Ethereum Improvement Proposal," which is typically followed by the assignment number of the standard (e.g., "EIP-20"), and which refers to a protocols and specifications design document for the Ethereum network. EIPs are typically related to core functionality of the Ethereum network, as opposed to application layer specifications.

ERC

An acronym for "Ethereum Request for Comment," which is typically followed by the assignment number of the standard (e.g., "ERC-20"), and which refers to a standardization document containing application layer specifications that programmers use to write Ethereum-based smart contracts. Different ERC standards have emerged with different primary use cases.

ERC-20

An ERC standard detailing the protocol for the issue and transfer and other aspects of fungible tokens on the Ethereum network.

ERC-721

One of the ERC standards used to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token), ERC-721 tokens are unique.

ERC-1155

An ERC standard for the specifications of a smart contract interface that can represent any number of fungible and non-fungible token types in single transactions.

Ether (ETH)

The native token used to operate the Ethereum platform. Ether provides the incentive for nodes to validate blocks on the Ethereum network that contain the smart contract code.

Ethereum

An open-source, public, blockchain-based distributed computing platform released on 30 July 2015 by Vitalik Buterin, featuring smart contract functionality that allows developers to build and deploy dApps.

Ff

Fiat currency

Money declared by a government to be legal tender (e.g., GBP or USD).

Fork

A fork is the creation of an ongoing alternative version of the blockchain, by creating two blocks simultaneously at a given block height. Forks occur naturally when two blocks are found simultaneously by competing miners. These types of forks resolve automatically when the next miners choose to build on top of only one of the branches formed. Forks may also be used to intentionally create a new set of rules governing the validity of blocks in a blockchain.

See **Hard fork** and **Soft fork**.

FUD

An acronym for "fear, uncertainty and doubt," being a jargon term used in the cryptoasset industry to describe propaganda tactics and the spread of disparaging information about a crypto project or token, especially a competing one.

Gg

Gas

A measurement roughly equivalent to computational steps for Ethereum. Every transaction on Ethereum is required to include a gas limit and a fee that the user is willing to pay per gas. Ether miners have the choice of including the transaction and collecting the fee or not.

Gas limit

The maximum amount of units of gas that the user is willing to spend on a transaction. The transaction must have enough gas to cover the computational resources needed to execute the code. All unused gas is refunded at the end of the transaction.

Gas price

The price that a user is willing to pay for a transaction in terms of GWei.

Genesis block

The first block of a blockchain. It is generally hardcoded into the software of the applications that use its blockchain.

GWei

Each Ether is divisible into 1018 sub-units, called Wei. 1 GWei = 1 gigaWei = 1 billion Wei, or 1 billionth of an Ether

Hh

Hard fork

A fork that can render previously invalid types of transactions valid, and vice versa. This type of fork requires all nodes and users to upgrade to the latest version of the protocol software. Therefore, a hard fork is a permanent change to the rules of the previous version of the blockchain, and nodes using the previous version will not recognize the new version. A hard fork may be implemented to correct security vulnerabilities, add new functionality or reverse transactions (see **DAO**). Bitcoin Cash is a hard fork of Bitcoin.

Hash

An identifier for input data that does not disclose information about the data. In essence, a hash function takes input data and returns a fixed-length value, which acts as a "digital fingerprint" for the input data. The hash will always be the same for the same input data.

Modifying the input data even by a tiny amount will change the hash in an unpredictable manner (see the example below). The consensus process securing the Bitcoin blockchain relies on data being hashed using the SHA-256 hashing algorithm.

The following examples of SHA-256 hashes demonstrate the unpredictable changes arising from even a slight change to the input:

Baker McKenzie: b27cb2ba88e38 dbec56ab4579996c29ab415aef1 f2b8c63b228970237e04edcb

Add an "a" to McKenzie and you get an entirely different hash.

Baker MacKenzie: 7c018bca881e1 39f6b862cdb9df8e21e622967ee5 0243ca3da765d4ae87fe8d6

Ii Initial coin offering (ICO)

An innovative form of crowdfunding. In an ICO, or token sale, a company sells digital tokens that are issued through DLT, typically in exchange for Ether or other cryptocurrencies. In a token sale, the tokens can perform different functions. For example, tokens may take the form of payment tokens, utility tokens or asset tokens.

Jj Just

...under halfway now — are you still with us?

Kk Keys

Public key cryptography uses public and private keys to encrypt and decrypt data. In the context of cryptocurrencies and, more specifically, Bitcoin, a private key is a secret number that relates to a user's Bitcoin address. The private key enables a user to spend Bitcoins as it generates a digital signature, mathematically confirming the user has the right to issue each transaction that they send out. The Bitcoins are sent to another user's public key address and become their property, because their private key cannot be identified from their public key.

Ll Layer 1 blockchain

Describes a blockchain network that is the fundamental blockchain network in its relevant ecosystem for on-chain transactions. As a defining feature, Layer 1 networks can validate and finalize transactions without the need for another network (e.g., the Bitcoin or Ethereum networks). Developers can create Layer 2 networks atop of Layer 1 networks, often done to improve transaction efficiencies or speed. The Bitcoin Lightning Network is an example of a Layer 2 network.

Ledger

A database that records transactions.

Legal smart contract

A type of smart contract that can be used to define and perform the obligations of a legally binding contract.

Mm

Metaverse

Science fiction author Neal Stephenson coined the term "metaverse" in his 1992 cyberpunk novel "Snow Crash." There is no market consensus on the meaning of metaverse as broadly used today, but references to a metaverse tend to be used to describe a digital environment that provides enhanced immersive experiences.

Mining

The process by which blocks of transactions are verified and added to a blockchain, typically by using a computer processor to solve a mathematical problem. Computers who solve these mathematical problems are known as "miners."

Minting

The process of creating new tokens in a blockchain network, typically used in reference to the creation of non-fungible tokens. In the context of NFTs, this term also incorporates the linking of digital content to non-fungible tokens on a blockchain network, as a means of creating a digital asset.

Nn

NFT

An NFT (non-fungible token) is a unique, noninterchangeable cryptographic token. NFTs are recorded and traded via blockchain technology, which tracks and certifies asset ownership.

Nick Szabo

The computer scientist credited with coining the term "smart contract."

Node

Any computer that connects to the DLT network. Nodes first connect to the network and obtain an up-to-date copy of the ledger. Each node is responsible for receiving, validating and relaying transactions and blocks to its peers. This security model (massive redundant distribution with mathematical validation by each participant) ensures permanent availability of data across the network and rejection of invalid transactions.

Nonce

In cryptography, an arbitrary string of numbers that can only be used once. The nonce is an important concept in proof-of-work mining, as used by Bitcoin, for example.

Oo

Off-chain

Activity that happens, or data that is stored, outside the blockchain ledger, but may be referenced from it.

Oracle

A trusted off-chain agent for a distributed ledger system that can submit information to be used by on-chain smart contracts. For example, an oracle might link to a third-party verified source of weather data, travel timetables, stock market information, registry information, or to a physical Internet of Things device.

Pp

Payment tokens

Digital tokens that enable the token holder to acquire goods or services from the token issuer (i.e., performs as virtual currency).

Permissioned

A DLT system where only pre-authorized nodes can finalize transactions into the ledger. Consortium blockchains are permissioned systems.

Permissionless

A DLT system where all nodes can access, submit and be selected to finalize transactions into the ledger.

Phygital

A term combining physical and digital (pronounced "fidge-it-al"). The concept of using technology to bridge the digital world with the physical world with the purpose of providing a unique interactive experience for the user.

POAP

An acronym for "Proof of Attendance Protocol." A POAP NFT is a type of NFT that shows that you attended a particular event or experience — a digital memento.

Pre-sale

Tokens are offered for sale to a limited set of participants before they are made available to the general public via an ICO.

Private blockchain/DLT

A blockchain/DLT that is only accessible to certain participants. Only pre-authorized nodes can access and submit transactions or finalize transactions. A private blockchain/DLT is always a permissioned blockchain/DLT.

Company blockchains are private systems.

Private key

A unique number that acts as a personal password to access cryptoassets in a specific wallet. The key is kept hidden from anyone but the owner of the wallet. Whoever has access to the private key effectively "owns" the cryptoassets.

Public blockchain/DLT

A blockchain/DLT system that permits anyone with a computer to create a node. A public blockchain can be permissioned or permissionless.

Proof-of-stake

An alternative to proof-of-work.

Mining requires a lot of computing power, which translates to high electricity usage. Proof-of-stake seeks to address this by limiting what you can mine to the stake of the particular cryptocurrency that you own (for example, if you own 1% of all Ether available, then you can only mine 1% of the blocks. This also mitigates the risk that miners create competing forks because this would devalue each miner's stake).

Proof-of-work

Proof-of-work involves using computer processing power to perform repeated hash operations with different nonce values to find a resulting hash below the required difficulty. Finding such a hash allows the miner to add a block of transactions to the chain tip of a growing blockchain. Those involved in mining ("miners") are incentivized to use their computing resources to mine by receiving block rewards. Because this is difficult and consumes large amounts of electricity, it is an effective way of securing the blockchain from attempted rewriting of history (e.g., to double-spend) or breaking consensus.

Public key

A cryptographic key used to encrypt messages. A user can "sign" data with their private key and anyone who knows the user's public key can verify that the signature is valid.

However, encrypted messages can be deciphered only by using the paired private key, which cannot be calculated from knowing the public key. A Bitcoin wallet address is a hashed version of the user's public key.

Qq

Quantum computing

Quantum computing is seen as a possible threat to the security of blockchain systems because quantum computers are expected to be able to make decrypting information encrypted using certain mathematical principles (such as prime factorization) far easier. These principles underpin many of the encryption methods (such as the SHA-256 hash) used in not only the blockchain industry, but also in securing information transmitted over the internet.

Rr

Regulatory sandbox

A controlled space set up by regulators, such as the UK's Financial Conduct Authority, to allow authorized and unauthorized firms to test innovative products services, business models and delivery mechanisms in the real market with real consumers.

Ss

Satoshi Nakamoto

The name used by the unknown person or persons who wrote Bitcoin's code in 2007 and authored the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System," which established the foundations for the Bitcoin protocol.

SHA-256 hash

A "Secure Hash Algorithm 2" function that produces 256-bit long output values. The cryptographic hash algorithm used in proof-of-work mining to secure Bitcoin and many other blockchain-based cryptocurrencies (notably not Ethereum, Monero, or Ripple).

Side chain

A blockchain that is connected to a parent (primary) blockchain and allows a user to use the cryptoassets securely within that blockchain, but also transfer cryptoassets to and from the parent blockchain.

Smart contract

The term "smart contract" is rather a misnomer. A smart contract is not typically a contract in the legal sense, although a smart contract could be used to automate elements of a legal contract. Smart contracts are programmable transactions — computer code that sits in an application layer on top of the distributed ledger and acts as an execution mechanism. When certain conditions are met, the protocols automatically execute a set of instructions.

Soft fork

Unlike a hard fork, in a soft fork, the fork is a software upgrade that is backwards-compatible, i.e., existing nodes will recognize the new code and still be able to function on the network, but cannot take advantage of the new features on offer. Because of this reduced functionality, soft forks incentivize those who have not upgraded to upgrade.

Stablecoin

A cryptoasset that purports to maintain a stable value relative to a specified asset, or a pool or basket of assets. Stablecoins can be backed by reserve assets, backed algorithmically by a smart contract or otherwise tied to some form of external asset. They may also be pegged to a specific fiat currency.

Tt

Timestamp

Each block contains a timestamp of when it was created. This provides an indication of when a transaction was added to the chain.

Token

Tokens are digital assets issued in connection with an application that uses an existing blockchain (such as Ethereum) and can take a variety of different forms. See **Asset tokens**, **Payment tokens** and **Utility tokens**.

Uu Utility tokens

A token that provides users with digital access to an application, product or service (think membership card).

Vv Verification

Transaction verification is a mathematical process of checking that a transaction submitted to a node is a permitted unique transfer of unspent value (see **Double-spending**) and that the correct private key has been used to sign the transaction. Block verification checks additional parameters involved in the consensus process, for example, that the block has been correctly mined and has an appropriate timestamp.

Ww Wallet

A storage device for the user's collection of private keys that communicates with the corresponding blockchain/DLT. Typically an online digital wallet (a software application), but can also be an offline hardware wallet. See **Cold storage**.

Web3

An envisaged version of the internet that is decentralized and based on peer-to-peer technologies, such as public blockchains, and decentralized participants, such as DAOs, and that incorporates digital assets and currencies in a token-based economy.

Whitepaper

In the context of ICOs or NFT offerings, an informational document that provides details on the philosophy, objectives and technology of a given project or initiative and is released in advance of the ICO or NFT issuance to attract interest.

Xx XRP

XRP is the native cryptocurrency of the Ripple platform. Unlike Bitcoin, XRP is pre-mined, i.e., it was all introduced at its inception.

Yy Yikes

With this much jargon, you can see why blockchain causes so much head-scratching.

Zz Zero knowledge proof

A cryptographic method by which one party can prove (the prover) to another party (the verifier) that they know secret information, without revealing the secret information (for example, by way of analogy, in the case of identity, being able to prove that you are over 21 without revealing your actual age or date of birth).

With digital transformation driving an unprecedented shift in financial institutions (FIs), we provide the full range of legal services FIs and fintech innovators need to develop and adopt products and services such as crowdfunding, e-payment platforms, cryptocurrencies, digital banking and peer-to-peer lending.

We advise clients on fintech matters including regulatory compliance, data protection, tax structuring, capital raising, consumer protection, commercial contracts, M&A, competition law, employment matters and more. Our years of experience acting for some of the world's largest and most innovative technology companies gives our fintech clients access to time-tested techniques and strategies.

Find out how we're helping financial institutions, technology providers and fintech innovators stay ahead of the game by visiting our **Fintech Hub** for more information.

Baker McKenzie is ranked Band 1 by Chambers for FinTech Global-wide.

"Baker McKenzie deals with international complexity very well. They provided us with consolidated and clear advice in crypto-related matters."

Client quote
Chambers FinTech Legal 2022